GeekBrains

Урок 5 Тема 1

Способы обхода активации программ

Реверс-инжиниринг

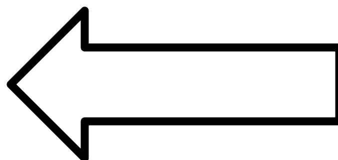
В этом видео

1. Продление триального периода.
2. Патчинг.
3. Создание ключа.
4. Перенаправление сетевых запросов.

Обход активации программ



Software Piracy



```
0040107B  .v  7D 11          JGE SHORT prog-3_3.0040108E
0040107D  .   68 0C904100    PUSH prog-3_3.0041900C
00401082  .   E8 99000000    CALL prog-3_3.00401120
00401087  .   83C4 04        ADD ESP,4
0040108A  .   33C0           XOR EAX,EAX
0040108C  .v  EB 41          JMP SHORT prog-3_3.004010CF
0040108E  >   B8 04000000    MOV EAX,4
00401093  .   C1E0 00        SHL EAX,0
00401096  .   8B4D 0C        MOV ECX,DWORD PTR SS:[EBP+C]
00401099  .   8B1401         MOV EDX,DWORD PTR DS:[ECX+EAX]
0040109C  .   52             PUSH EDX
0040109D  .   E8 5EFFFFFF    CALL prog-3_3.00401000
004010A2  .   83C4 04        ADD ESP,4
004010A5  .   8945 FC        MOV DWORD PTR SS:[EBP-4],EAX
004010A8  .   817D FC E803   CMP DWORD PTR SS:[EBP-4],3E8
004010AF  .v  75 0F          JNZ SHORT prog-3_3.004010C0
004010B1  .   68 30904100    PUSH prog-3_3.00419030
004010B6  .   E8 65000000    CALL prog-3_3.00401120
004010BB  .   83C4 04        ADD ESP,4
004010BE  .v  EB 0D          JMP SHORT prog-3_3.004010CD
004010C0  >   68 4C904100    PUSH prog-3_3.0041904C
004010C5  .   E8 56000000    CALL prog-3_3.00401120
004010CA  .   83C4 04        ADD ESP,4
004010CD  >   33C0           XOR EAX,EAX
004010CF  >   8BE5           MOV ESP,EBP
004010D1  .   5D             POP EBP
004010D2  .   C3             RETN
```

Способы обхода активации программ

- Продление триального периода.
- Создание ключа.
- Патчинг.
- Перенаправление сетевых запросов.

GeekBrains

Продление триального периода



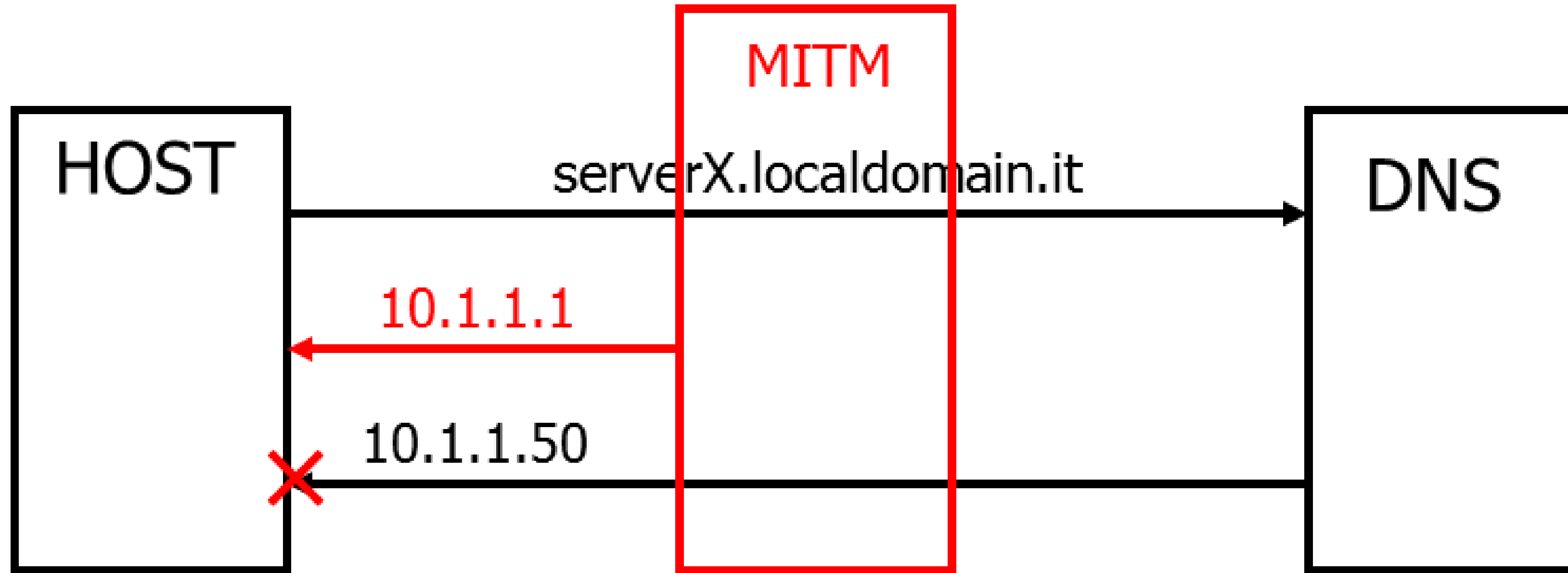
Создание ключа

Патчинг

- Патчинг PE-файла.
- Патчинг образа PE-файла в виртуальной памяти.



Перенаправление сетевых запросов



Итоги

1. Познакомились со способами обхода активации программ.
2. Узнали преимущества и недостатки рассмотренных способов.